Deutscher Bundestag **Drucksache 17/7118**
17. Wahlperiode 04. 10. 2011

Kleine Anfrage

der Abgeordneten Andrej Hunko, Wolfgang Gehrcke, Jan van Aken, Ulla Jelpke, Harald Koch, Kathrin Vogler, Halina Wawzyniak und der Fraktion DIE LINKE.

Cyber-Übungen der Europäischen Union, der USA und die deutsche Beteiligung

Am 4. November letzten Jahres hatte die Europäische Union ihre erste europäische Cyber-Übung „Cyber Europe 2010“ begonnen, um eine Reaktion auf „Onlinebedrohungen“ zu testen. 22 Mitgliedstaaten beteiligten sich, die Übung wurde vom European Network and Information Security Agency (ENISA) mit Sitz in Athen organisiert. Mit den Übungen soll die ENISA an der Verbesserung einer „Abwehrbereitschaft der EU“ arbeiten und hierfür laut einer Mitteilung des Ausschusses Ständiger Vertreter (AStV) zur „Robustheit und Stabilität des Internets, zum Aufbau strategischer internationaler Partnerschaften und zur Einbringung koordinierter Beiträge in internationalen Foren“ beitragen (Ratsdokument 10299/11). Chef der ENISA ist Udo Helmbrecht, früherer Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Übungen wie „Cyber Europe“ adressieren auch Cyberkriminalität. Unklar bleibt, welche konkreten „Störungen“ außer „Distributed Denial of Service Attacks“ (DDoS) im Mittelpunkt stehen und welcher Art die Antworten von Behörden und Privatwirtschaft darauf sind. In einer Mitteilung vom 31. März 2011 zum „Schutz kritischer Informationsinfrastrukturen ‚Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit‘“ spricht die Europäische Kommission (im Folgenden: Kommission) von der Nutzung von Informations- und Kommunikationstechnologie (IKT) zur Erlangung „politischer, wirtschaftlicher und militärischer Macht“ bzw. „Cyberkrieg“ und „Cyberterrorismus“. Indes hat es bislang – soweit bekannt – noch keinen „cyberterroristischen“ Angriff gegeben.

Im Ratsdokument 10299/11 wird neben einer „nationalen, europäischen und globalen Kultur der Risikoanalyse und des Risikomanagements auf allen Ebenen“ die Entwicklung „koordinierter Maßnahmen zur Prävention, Erkennung und Eindämmung von Störungen aller Art und zur entsprechenden Reaktion“ genannt. EU-Mitgliedstaaten sollen „einander bei grenzüberschreitenden Sicherheitsvorfällen auf freiwilliger Basis“ gegenseitig Hilfe leisten. Gegenüber dem Internetportal www.heise.de äußerte ENISA-Chef Helmbrecht, mögliches Szenario einer zukünftigen „Cyber Europe“ seien „Angriffe auf das Netz am Bankenplatz in Frankfurt“.

Im April 2011 hatte die Kommission in Balatonfüred eine Ministerkonferenz über den „Schutz kritischer Informationsinfrastrukturen“ veranstaltet, deren Ergebnisse der Ratsarbeitsgruppe „Telekommunikation und Informationsgesellschaft“ berichtet wurden. Gefordert wurde, die ENISA „rasch zu reformieren, zu modernisieren und zu verstärken“. Hierfür sollen vor allem die nationalen „IT Notfalldienste“ (Computer Emergency Response Teams – CERT) koordiniert werden, die sich zum großen Teil aus der Privatwirtschaft rekrutieren.

Nahtlos werden dadurch die beteiligten Firmen in die „Ausarbeitung nationaler Notfallpläne für Netzstörungen sowie der Veranstaltung von nationalen Übungen zur Internetsicherheit“ integriert, um neben einer „Generierung von Wachstum“ auch zur „Wettbewerbsfähigkeit“ und „Schaffung von Arbeitsplätzen“ beizutragen. In Deutschland werden CERT unter anderem von einigen Bundesländern, aber auch der Bundeswehr, dem BSI, der Volkswagen AG, der Commerzbank AG, IBM, SAP, der Siemens AG und der Telekom Deutschland GmbH betrieben.

Kurz vor der „Cyber Europe 2010“ hatten mehrere EU-Mitgliedstaaten (Frankreich, Deutschland, Ungarn, Italien, Niederlande, Schweden und Großbritannien) an der dritten zivil-militärischen US-Übung „Cyber Storm“ teilgenommen, die vom Ministerium für Innere Sicherheit der Vereinigten Staaten (DHS) geleitet wurde. Ebenfalls beteiligt waren Australien, Kanada, Japan und Neuseeland. Die Europäische Kommission und ENISA nahmen als Beobachter teil. Das DHS lobte die Übung als einzigartig, da noch mehr Akteure der Privatwirtschaft (60 Firmen) als zuvor beteiligt waren. Am „Cyber Storm III“ arbeiteten das „Department of Defense“, das „Defense Cyber Crime Center“, das „Office of the Joint Chiefs of Staff National Security Agency“, das „United States Cyber Command“ und das „United States Strategic Command“ mit. „Cyber Storm III“ testete das 2009 eröffnete „National Cybersecurity and Communications Integration Center“ (NCCIC).

Verabredet wurde nach Auswertung der „Cyber Storm III“, zukünftig gemeinsame Übungen mit den Mitgliedstaaten der EU abzuhalten. Demnach soll die Kommission 2011 mit den USA in einer neu eingerichteten „high-level EU-US Working Group on cyber security and cybercrime“ (MEMO/10/597) ein „gemeinsames Programm und einen Fahrplan für gemeinsame/abgestimmte transkontinentale Übungen zur Internetsicherheit in den Jahren 2012/2013“ entwickeln (Ratsdokument 8548/11). Weitere „Optionen für die Zusammenarbeit mit anderen Regionen oder Ländern“ sollen „erwogen“ werden.

Auf ihrer Sitzung am 14. April 2011 in Gödöllo kamen die Innen- und Justizministerinnen und -minister überein, noch dieses Jahr eine gemeinsame „EU-US cyber-incident exercise“ auszurichten (MEMO/11/246). Wieder sind eine starke Einbindung des „Privatsektors“ und die Beteiligung der „Industrie“ vorgesehen. Szenarien würden demnach eine „Bekämpfung von Botnetzen“ oder die „Verbesserung der Widerstandsfähigkeit und Stabilität des Internets“ sein. Bewusstseinsbildung wie Herangehensweisen sollen demnach vermehrt „über den Atlantik hinweg“ organisiert werden. Anhand von Webseiten mit kinderpornographischem Inhalt soll die EU-/US-Kooperation bei der „Entfernung“ von Webseiten entwickelt werden, darunter auch durch die Arbeit zusammen mit Anbietern von Domainregistrierung. Hierzu gehört ebenso noch 2011 eine Konferenz über „child protection online“ in Silicon Valley.

Wir fragen die Bundesregierung:

1. Welche EU-Behörden nehmen mit welchem Personal an der 2010 gegründeten „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ (High-level EU-US Working Group on cyber security and cybercrime) teil?

   a) Welche ähnlichen bilateralen Gespräche oder Initiativen finden zwischen der EU und welchen anderen Regierungen hierzu statt?

   b) Welche „neuen Bedrohungen“ soll die „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ konkret adressieren?

   c) Welche deutschen Behörden sind mit welchem Personal in der „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ organisiert?

d) Welche Ministerien, Behörden oder sonstigen Institutionen sind seitens der USA an der Arbeitsgruppe beteiligt?

e) Welche Zusammenarbeit mit anderen Regionen oder Ländern wurde bislang erwogen bzw. verabredet?

f) Welche Sitzungen der „high-level EU-US Working Group on cyber security and cybercrime“ haben seit ihrer Gründung mit welcher Tagesordnung stattgefunden?

g) Welche Plenartagungen oder Unterarbeitsgruppen werden innerhalb der „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ organisiert?

h) Welche Inhalte eines „Fahrplans für gemeinsame/abgestimmte transkontinentale Übungen zur Internetsicherheit in den Jahren 2012/2013“ hat die Arbeitsgruppe bereits entwickelt?

i) Innerhalb welcher Treffen hat sich die „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ seit ihrem Bestehen auch mit dem Thema „Bekämpfung von kriminellen Inhalten auf Webseiten“ oder „Kinderpornographie“ beschäftigt, und mit welchem Inhalt bzw. Ergebnis?

2. Welche Tagesordnungspunkte wurden auf dem jüngsten „EU-/US-Senior-Officials-Treffen“ behandelt, und wie wurde dort das Thema „Cyberkriminalität“ adressiert?

a) Welche Diskussionen wurden hinsichtlich eines „IP-Adressenmissbrauchs“ geführt, und wie ist die Haltung der Bundesregierung hierzu?

b) Welche Diskussionen wurden hinsichtlich der Bekämpfung von Kinderpornographie geführt, und wie ist die Haltung der Bundesregierung hierzu?

c) Welche Verabredungen wurden auf dem „EU-/US-Senior-Officials-Treffen“ getroffen, und welche weiteren Treffen sind 2011 vorgesehen?

3. Welche Regierungen von EU-Mitgliedstaaten sowie anderer Länder waren an der „Cyberstorm III“ aktiv beteiligt, und welche hatten eine beobachtende Position inne?

a) Welche US-Ministerien bzw. -Behörden waren an „Cyberstorm III“ beteiligt?

b) Wie ist das Verhältnis von zivilen zu staatlichen Akteuren bei Cyberstorm III?

c) Welche privaten Firmen bzw. sonstigen zivilgesellschaftlichen Akteure haben an „Cyberstorm III“ teilgenommen?

d) Wie bewertet die Bundesregierung die starke militärische Beteiligung bei der „Cyberstorm III“?

e) Wie war die Übung strukturell angelegt, und welche Szenarien wurden durchgespielt?

f) Wie viele Angehörige welcher deutscher Behörden haben an welchen Standorten teilgenommen?

g) Wie viele Personen haben insgesamt an der „Cyberstorm III“ teilgenommen?

h) Welche Kosten sind der Bundesregierung bei der Teilnahme entstanden?

4. Welche europäischen Länder waren an der „Cyber Europe 2010“ aktiv beteiligt, und welche hatten eine beobachtende Position inne?

a) Wie war die Übung strukturell angelegt, und welche Aufgabe erfüllte das zentrale Lagezentrum in Athen?

b) Welche weiteren „Experten von über 70 Einrichtungen des öffentlichen Bereichs und Behörden aus ganz Europa“ waren beteiligt?

c) Wie viele Angehörige welcher deutschen Behörden haben an welchen Standorten an der „Cyber Europe 2010“ teilgenommen?

d) Welche Szenarien wurden für die Übung angenommen und durchgespielt, und was ist unter den in der Pressemitteilung des ENISA vom 10. November 2010 gemeldeten 320 „Sicherheitsinjektionen“ zu verstehen?

e) Welche Kosten sind der Bundesregierung bei der Teilnahme entstanden, und aus welchen Etats wurden sie bestritten (bitte unter Angabe des prozentualen Anteils an den Gesamtkosten)?

5. Welche Vorbereitungen werden von Behörden der EU-Mitgliedstaaten für die Ausrichtung einer „Cyber Europe 2012“ unternommen?

   a) Welche europäischen sowie nichteuropäischen Akteure werden nach derzeitigem Stand teilnehmen bzw. sind an Vorbereitungen beteiligt?

   b) Welche Rolle spielt der innerhalb der „Cyber Europe 2012“ zu testende „Europäische Mechanismus zur Zusammenarbeit bei Netzstörungen“, und was ist darunter zu verstehen?

6. Welche Aktivitäten oder Übungen sind im Zusammenhang mit dem „EuroCybex-Projekt“ geplant?

   a) Welche Behörden und privaten Akteure welcher EU-Mitgliedstaaten sind in das „EuroCybex-Projekt“ integriert?

   b) Welche nichteuropäischen Akteure sind darüber hinaus auf welche Art und Weise beteiligt?

7. Welchen Inhalt hatte die in Budapest ausgetragene Konferenz zu „Cybercrime“ vom 12. bis 13. April 2011?

   a) Welche Ministerien bzw. Behörden welcher Länder haben an der Konferenz teilgenommen?

   b) Mit welchem Personal waren deutsche öffentliche und private Einrichtungen beteiligt?

   c) Welche Vertreter welcher US-Behörden haben mit welchem Anliegen an der Konferenz teilgenommen?

   d) Welche weiteren privaten Akteure waren auf besagter Konferenz präsent?

   e) Welche konkreten Verabredungen wurden im Rahmen der auf der Konferenz erörterten „Vertiefung der praktischen Zusammenarbeit der Strafverfolgungsbehörden“ getroffen?

8. Welche weiteren Erläuterungen hat die frühere ungarische Ratspräsidentschaft bezüglich ihres im April 2011 in der Ratsarbeitsgruppe Strafverfolgung vorgebrachten Vorschlags eines „single secure European cyberspace“ gemacht, und falls diese nicht vorgelegt wurden, mit welchem Fortgang der Initiative rechnet die Bundesregierung?

9. Welche Haltung vertritt die Bundesregierung in den Verhandlungen um die Richtlinie des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme bezüglich des Strafmaßes für die von dem Vorschlag erfassten Grundtatbestände, die erschwerenden Umstände und die Vorschriften für die gerichtliche Zuständigkeit?

a) Der Besitz oder Betrieb welcher „Vorrichtungen“ soll nach gegenwärtigem Stand in der Richtlinie kriminalisiert werden?

b) Wie sind bislang „minderschwere Fälle“ definiert?

c) Welche Position vertritt die Bundesregierung hinsichtlich einer „Anstiftung zu Cybercriminalität“, und wie ist diese in der deutschen Strafprozessordnung geregelt?

d) Welche Position vertritt die Bundesregierung hinsichtlich eines „Internet Kill Switch“?

10. Welche Behörden, privaten Akteure oder sonstigen Institutionen haben in Deutschland CERT aufgebaut, und welche konkreten Ziele und Zwecke werden damit jeweils verfolgt?

11. Welche EU-Mitgliedstaaten haben der Bundesregierung nationale bzw. private CERT gemeldet, bzw. mit welchen weiteren ausländischen CERT arbeiten deutsche Behörden zusammen?

    Welche weiteren CERT sind für weitere EU-Institutionen bis 2012 vorgeschlagen, und wie sind sie bislang umgesetzt?

12. Welche Absicht wird mit den „Operational Action Plans“ (OAP) verfolgt, die innerhalb des von der früheren belgischen Ratspräsidentschaft begonnenen „Policy Cycle“ eingerichtet wurden?

    a) Welche Inhalte sollen in den zukünftigen OAP „Cyberkriminalität“ behandelt werden, und welche Initiativen wären vermutlich damit verbunden?

    b) Wie kam die Entscheidung zustande, der rumänischen Delegation die Federführung der OAP zu überlassen, bzw. welche Ausführungen hatte diese zuvor dazu gemacht?

    c) Wie ist die Polizeiagentur Europol in die Umsetzung der OAP eingebunden?

13. Welchen Stand haben die Verhandlungen um die Erweiterung des Mandates der ENISA?

    Welche EU-Mitgliedstaaten bzw. anderen Regierungen wurden 2010 und 2011 von der ENISA unterstützt, nationale Notfallpläne aufzustellen oder Übungen durchzuführen?

14. Wie beteiligt sich die Bundesregierung am Aufbau eines „Europäischen Informations- und Warnsystems“ (EISAS)?

    a) Welche Stellen innerhalb der EU sollen an das EISAS angeschlossen sein?

    b) Wen soll das EISAS mit zukünftigen Informationen beliefern?

15. Welche Behörden bzw. Abteilungen der Bundesregierung sowie deutschen privaten Akteure sind in der „Europäischen öffentlich-privaten Partnerschaft für Robustheit“ (EP3R) organisiert?

    a) Was ist unter den dort formulierten „Zielen für Sicherheit und Robustheit“ sowie „bewährten Maßnahmen“ zu verstehen?

    b) Mit welchen „Partnern aus Drittländern“ bzw. welchen ihrer Behörden oder privaten Akteuren wird innerhalb der EP3R zusammengearbeitet?

    c) Wie ist die ENISA in den Aufbau bzw. die Tätigkeit der EP3R eingebunden?

    d) Nach welchem Verfahren wurden Ziele, Grundsätze und Aufbau der EP3R festgelegt?

e) Wie ist die EP3R in die „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ eingebunden?

16. Welche Behörden bzw. Abteilungen der Bundesregierung sowie deutscher privater Akteure sind im „Europäischen Forum der Mitgliedstaaten“ (EFMS) vertreten?

a) Auf welche Art und Weise arbeitet das EFMS mit der ENISA zusammen?

b) Welche Rolle spielt das EFMS bei der Ausgestaltung von Cyber-Übungen?

c) Welche konkreten „technischen Erörterungen“ sind hierfür bislang verfasst worden?

d) Wie ist das EFMS in die internationale Zusammenarbeit integriert?

e) Welche Ziele und Zwecke werden mit der Tätigkeit des EFMS in der „Arbeitsgruppe EU – USA zum Thema Cybersicherheit und Cyberkriminalität“ verfolgt?

f) Welche „Bewertung des Grades der Cybersicherheit in Europa“ hat das EFMS 2010 und 2011 analysiert, und wie wurde diese ermittelt?

17. Mit welchen „internationalen Partnern“, insbesondere aus den USA, der G8 und der OECD, hat die Europäische Kommission 2011 die „Grundsätze und Leitlinien für die Robustheit und Stabilität des Internets“, wie in der „Mitteilung über den Schutz kritischer Informationsinfrastrukturen – Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit“ vom 31. März 2011 beschrieben, erörtert?

Welche Ergebnisse zeitigte die weitere Erörterung „mit relevanten Akteuren, insbesondere des Privatsektors“, und welche sind hiermit konkret gemeint?

18. Inwieweit sind welche deutschen Behörden oder privaten Akteure in die in London gestartete „International Cyber Security Protection Alliance“ (ICSPA) eingebunden?

a) Von welchen EU-Institutionen bzw. -Regierungen wird die Initiative finanziert?

b) Mit welchen Arbeitsgruppen und Aufgaben nimmt die EU-Polizeiagentur EUROPOL an der ICSPA teil?

19. Welche Erkenntnisse hat die Bundesregierung darüber, wo es bis heute einen versuchten oder erfolgreich ausgeführten „cyberterroristischen Anschlag“ gegeben hat?

a) Würde die Bundesregierung das Auftauchen von „Stuxnet“ als „cyberterroristischen Anschlag“ kategorisieren?

b) Falls es bislang keine bekannten „cyberterroristischen Anschläge“ gegeben hat, auf welche Annahmen oder wenigstens Risikoanalysen gründen sich die zahlreichen EU-Verlautbarungen und Forderungen (unter anderem des EU-Anti-Terrorismuskoordinators) zur Bekämpfung derselben?

c) Über welche Studien bzw. Risikoanalysen verfügt die Bundesregierung bezüglich der Wahrscheinlichkeit eines größeren Ausfalls von Informationsinfrastrukturen?

d) Über welche Studien bzw. Risikoanalysen verfügt die Bundesregierung bezüglich der Wahrscheinlichkeit einer Zerstörung kritischer Infrastruktur durch digitale Angriffe?

20. Welches Szenario liegt der diesjährigen „Länder Übergreifenden Krisenmanagementübung (Xercise)“ (LÜKEX) vom 30. November bis 1. Dezember 2011 zugrunde?

    a) Welche Krisenstäbe des Bundes und der Länder werden sich hierfür mit welchen Lagezentren beteiligen?

    b) Wer ist verantwortlich für das Erstellen bzw. den Inhalt fiktiver TV-Sendungen, Presseberichte und -kommentare sowie Anfragen von Journalisten?

    c) Inwieweit berücksichtigt die Übung auch „cyberterroristische Anschläge“ oder sonstige über das Internet ausgeführte Angriffe auf Kritische Infrastruktur?

    d) Welche ausländischen privaten oder öffentlichen Stellen sind in die Übung integriert oder beobachten diese?

21. Entspricht die Erklärung vom Ministerialrat und Referatsleiter im Bundesministerium der Verteidigung, Horst Stern, auf der Tagung der Bundesakademie für Sicherheitspolitik „Auf dem Weg zur Automatisierung und Digitalisierung des Krieges?“ am 11. November 2010 „[…] Alle Versuche, eine Gesellschaft, ihren Staat oder ihre wirtschaftlichen Verhältnisse zu ändern sind politisch. Hier ist die Bundeswehr einzusetzen“ der Haltung der Bundesregierung, und falls nein, wie wird sie diese Darstellung korrigieren?

22. Wie steht die Bundesregierung zum Vorschlag des polnischen Ratsvorsitzes, einer potentiellen „cyberterroristischen Bedrohung“ auf EU-Ebene mittels Erstellung eines übergreifenden „Glossars“ zu begegnen, innerhalb dessen die Praktiken von Cyberabwehrstrukturen der Mitgliedstaaten evaluiert werden?

    a) Welche Haltung vertritt der EU-„Anti-Terrorismuskoordinator“ hierzu, und wie begründet er diese in den zuständigen Ratsarbeitsgruppen gegenüber Delegationen der Bundesregierung?

    b) Wie bewertet die Bundesregierung die Absicht, im Glossar eine aus NATO-Strategien übernommene Formulierung zur bestehenden Gefahr „cyberterroristischer“ Anschläge aufzunehmen, obschon es bislang weltweit noch keinen bekannten „cyberterroristischen“ Angriff gegeben hat?

23. Wie ist der Europäische Auswärtige Dienst, der EU-Militärstab (mit seinem „Capability developement plan“) oder die NATO (mit ihrem „Strategic Concept on Cybersecurity“) in die konkrete Ausgestaltung übergreifender Konzepte zur Cybersicherheit in der EU beteiligt?

Berlin, den 4. Oktober 2011

Dr. Gregor Gysi und Fraktion



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333